What is claimed is:

CLAIMS

1. A method of performing encrypted WLAN (Wireless Local Area Network) communication, comprising the steps of:

performing a connection set-up for said encrypted WLAN communication; and

performing data frame encapsulation and/or decapsulation during said encrypted WLAN communication;

wherein said connection set-up is performed by executing software-implemented instructions; and

wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware.

2. The method of claim 1, wherein the step of performing said connection set-up comprises authenticating a WLAN station by another WLAN station and/or a WLAN authentication server.

3. The method of claim 1, wherein the step of performing said connection set-up comprises associating a WLAN station with another WLAN station and/or a WLAN access point as WLAN communication counter-parts.

4. The method of claim 1, wherein the step of performing said connection set-up comprises exchanging cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point.

5. The method of claim 1, wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software.

6. The method of claim 5, wherein the step of obtaining the plurality of data frames comprises obtaining a plurality of data frames comprising cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation.

7. The method of claim 6, wherein said determining factor comprises a way in which a data frame intended for the data frame encapsulation is fragmented.

8. The method of claim 6, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation.

9. The method of claim 6, wherein said determining factor comprises a cryptographic key suitable for encrypting a data frame.

10. The method of claim 5, wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a prioritization algorithm implemented on the single-purpose hardware.

11. The method of claim 5, wherein the step of performing said data frame encapsulation comprises inserting a package number and/or sequence number into one of the plurality of data frames.

12. The method of claim 5, wherein the step of performing said data frame encapsulation comprises encrypting at least part of one of the plurality of data frames.

13. The method of claim 5, wherein the step of performing said data frame encapsulation comprises calculating an integrity value appropriate for verifying integrity of one of the plurality of data frames once said data frame decapsulation is completed.

14. The method of claim 13, wherein the step of performing said data frame encapsulation comprises encrypting said integrity value.

15. The method of claim 14, wherein the step of performing said data frame encapsulation comprises inserting the encrypted integrity value into one of the plurality of data frames.

16. The method of claim 1, wherein performing said encrypted WLAN communication further comprises receiving a data frame intended for said data frame decapsulation from a WLAN station and/or WLAN access point.

17. The method of claim 1, wherein the step of performing said data frame decapsulation comprises obtaining cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation from a storage unit within the single-purpose hardware.

18. The method of claim 17, wherein said determining factor comprises a cipher protocol suitable for performing the data frame decapsulation.

19. The method of claim 17, wherein said determining factor comprises a cryptographic key suitable for decrypting a data frame.

20. The method of claim 16, wherein the step of performing said data frame decapsulation comprises decrypting at least part of the data frame.

21. The method of claim 20, wherein the data frame comprises an encrypted integrity value appropriate for verifying integrity of the data frame once said data frame decapsulation is completed, and the step of decrypting at least part of the data frame comprises decrypting the encrypted integrity value.

22. The method of claim 21, wherein the step of performing said data frame decapsulation further comprises calculating the integrity value from at least part of the data frame except the encrypted integrity value.

23. The method of claim 22, wherein the step of performing said data frame decapsulation further comprises calculating an integrity verification value indicating a difference between the decrypted integrity value and the calculated integrity value.

24. The method of claim 23, wherein the step of performing said data frame decapsulation further comprises inserting said integrity verification value into the data frame.

25. The method of claim 24, wherein performing said encrypted WLAN communication further comprises performing counter-measures according to said integrity verification value by executing software-implemented instructions, wherein said counter-measures are suitable for limiting the amount of information available to an illegitimate WLAN protruder.

26. The method of claim 1, wherein the step of performing said data frame encapsulation and/or decapsulation comprises generating cryptographic data suitable for encrypting or decrypting a data frame.

27. The method of claim 26, wherein the step of generating cryptographic data comprises generating authentication data suitable for encrypting a data frame in a manner specific to a WLAN station or decrypting a data frame encrypted in a manner specific to a WLAN station.

28. The method of claim 1, wherein said encrypted WLAN communication is performed based on the IEEE 802.11i security standard.

29. The method of claim 1, wherein said encrypted WLAN communication is performed in a WLAN based on the IEEE 802.11b standard.

30. The method of claim 1, wherein said software-implemented instructions are executed on general-purpose hardware by driver software.

31. The method of claim 1, wherein said single-purpose hardware is operated periodically.

32. The method of claim 31, wherein said single-purpose hardware is operated periodically at 11MHz.

33. The method of claim 31, wherein said data frame encapsulation and/or decapsulation is performed according to the TKIP (Temporal Key Integrity Protocol) protocol.

34. The method of claim 33, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing RC4 (Rivest's Cipher 4) encryption and/or decryption.

35. The method of claim 34, wherein said RC4 encryption and/or decryption is performed by operating at least part of the single-purpose hardware.

36. The method of claim 35, wherein said part of the single-purpose hardware has a tree structure.

37. The method of claim 36, wherein said RC4 encryption and/or decryption is performed by operating only a sub-part of the single-purpose hardware corresponding to the tree root, part of the tree leaves and the tree components interconnecting the tree root with said part of the tree leaves.

38. The method of claim 37, wherein said sub-part of the single-purpose hardware corresponds to the tree root, two of the tree leaves and the tree components interconnecting the tree root with said two of the tree leaves.

39. The method of claim 34, wherein the step of performing said RC4 encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and said RC4 encryption and/or decryption is split over at least two operating periods of the

single-purpose hardware to encrypt or decrypt one byte of the data frame.

40. The method of claim 31, wherein said data frame encapsulation and/or decapsulation is performed according to the CCMP (Counter-mode Cipher block chaining Message authentication code Protocol) protocol.

41. The method of claim 40, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing CCMP-AES (Advanced Encryption Standard) encryption and/or decryption.

42. The method of claim 41, wherein the step of performing said CCMP-AES encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and said CCMP-AES encryption and/or decryption is performed by repeatedly performing a sequence of encryption or decryption steps on said part of the data frame.

43. The method of claim 42, wherein the step of performing the sequence of encryption or decryption steps comprises performing byte substitution using a plurality of cryptographic substitution boxes.

44. The method of claim 43, wherein the step of performing byte substitution on said part of the data frame comprises sequentially performing the byte substitution on a plurality of sub-parts of said part of the data frame.

45. The method of claim 42, wherein the step of performing the sequence of encryption or decryption steps is split over at least two operating periods of the single-purpose hardware.

46. A single-purpose hardware device for performing data frame encapsulation and/or decapsulation during encrypted WLAN (Wireless Local Area Network) communication, comprising:

internal hardware components; and

an interface for communicating with an external hardware component configured to perform a connection set-up for the encrypted WLAN communication by executing software-implemented instructions;

wherein said internal hardware components comprise internal single-purpose hardware components for performing the data frame encapsulation and/or decapsulation once the connection set-up is completed.

47. The single-purpose hardware device of claim 46, wherein said internal hardware components further comprise an internal memory for storing data frames intended for or resulting from the data frame encapsulation or decapsulation.

48. The single-purpose hardware device of claim 47, wherein said internal memory comprises an arbitration unit for performing memory access control.

49. The single-purpose hardware device of claim 47, wherein said internal memory comprises a hash memory for storing cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation.

50. The single-purpose hardware device of claim 49, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation and/or decapsulation.

51. The single-purpose hardware device of claim 49, wherein said determining factor comprises a cryptographic key suitable for encrypting or decrypting a data frame.

52. The single-purpose hardware device of claim 47, wherein said internal hardware components further comprise a radio transceiver for

receiving data frames from and/or transmitting data frames to a WLAN station and/or WLAN access point.

53. The single-purpose hardware device claim 52, wherein said internal single-purpose hardware components comprise a cryptographic component for performing the data frame encapsulation and/or decapsulation and a MAC (Medium Access Control) component for communicating with the radio transceiver.

54. The single-purpose hardware device of claim 53, wherein said cryptographic component and said internal memory are arranged to communicate with each other.

55. The single-purpose hardware device of claim 53, wherein said cryptographic component and said MAC component are arranged to communicate with each other.

56. The single-purpose hardware device of claim 53, wherein said MAC component and said internal memory are arranged to communicate with each other.

57. The single-purpose hardware device of claim 53, wherein said internal memory is arranged to communicate, over the interface, with the external hardware component.

58. The single-purpose hardware device of claim 53, wherein said MAC component further is for performing a prioritization algorithm for selecting a data frame for said data frame encapsulation from a plurality of data frames.

59. The single-purpose hardware device of claim 46, wherein at least one of said internal single-purpose hardware components is capable of inserting a packet number and/or sequence number into a data frame.

60. The single-purpose hardware device of claim 46, wherein at least one of said internal single-purpose hardware components is capable of

generating cryptographic data suitable for encrypting or decrypting a data frame.

61. The single-purpose hardware device of claim 60, wherein said at least one of the internal single-purpose hardware components is capable of generating cryptographic data comprising authentication data suitable for encrypting a data frame in a manner specific to a WLAN station or decrypting a data frame encrypted in a manner specific to a WLAN station.

62. The single-purpose hardware device of claim 46, wherein said internal single-purpose hardware components are for performing the data frame encapsulation and/or decapsulation according to the TKIP (Temporal Key Integrity Protocol) protocol;

wherein at least part of the internal single-purpose hardware components further is for performing RC4 (Rivest's Cipher 4) encryption and/or decryption; and

wherein said part of the internal single-purpose hardware components is adapted to perform the RC4 encryption and/or decryption on at least part of a data frame comprising bytes.

63. The single-purpose hardware device of claim 62, wherein said part of the internal single-purpose hardware components has a tree structure; and

wherein said part of the internal single-purpose hardware components is further adapted to perform the RC4 encryption and/or decryption on one byte by operating only a sub-part of said part of the internal single-purpose hardware components, said sub-part corresponding to the tree root, part of the tree leaves and the tree components interconnecting the tree root with said part of the tree leaves.

64. The single-purpose hardware device of claim 63, wherein said sub-part of said part of the internal single-purpose hardware components

corresponds to the tree root, two of the tree leaves and the tree components interconnecting the tree root with said two of the tree leaves.

65. The single-purpose hardware device of claim 62, wherein said single-purpose hardware device is operated periodically; and

wherein said part of the internal single-purpose hardware components is adapted to perform the RC4 encryption and/or decryption on one byte by splitting the RC4 encryption and/or decryption over at least two operating periods of said single-purpose hardware device.

66. The single-purpose hardware device of claim 46, wherein said internal single-purpose hardware components are for performing the data frame encapsulation and/or decapsulation according to the CCMP (Counter-mode Cipher block chaining Message authentication code Protocol) protocol;

wherein at least part of the internal single-purpose hardware components further is for performing CCMP-AES (Advanced Encryption Standard) encryption and/or decryption on at least part of a data frame comprising bytes by repeatedly performing on said part of the data frame a sequence of encryption and/or decryption steps comprising byte substitution; and

wherein said part of the internal single-purpose hardware components comprises a plurality of cryptographic substitution boxes for performing the byte substitution.

67. The single-purpose hardware device of claim 66, wherein said plurality of cryptographic substitution boxes is adapted to perform the byte substitution on said part of the data frame by sequentially performing the byte substitution on sub-parts of said part of the data frame.

68. The single-purpose hardware device of claim 66, wherein said single-purpose hardware device is operated periodically; and

wherein said internal single-purpose hardware components are adapted to perform the sequence of encryption and/or decryption steps by splitting said sequence over at least two operating periods of the single-purpose hardware device.

69. An integrated circuit chip for performing data frame encapsulation and/or decapsulation during encrypted WLAN (Wireless Local Area Network) communication, comprising:

internal integrated circuits; and

at least one data bus for communicating with an external CPU (Central Processing Unit) configured to perform a connection set-up for the encrypted WLAN communication by executing software-implemented instructions;

wherein said internal integrated circuits comprise internal single-purpose integrated circuits for performing the data frame encapsulation and/or decapsulation once the connection set-up is completed.

70. A computer program product for performing encrypted WLAN (Wireless Local Area Network) communication, comprising:

computer program means for performing a connection set-up for said encrypted WLAN communication; and

computer program means for communicating, over an interface, with a single-purpose hardware device capable of performing data frame encapsulation and/or decapsulation during the encrypted WLAN communication;

wherein said connection set-up is performed by executing software-implemented instructions.

71. A computer system for performing encrypted WLAN (Wireless Local Area Network) communication, comprising:

first means for performing a connection set-up for said encrypted WLAN communication; and

second means for performing data frame encapsulation and/or decapsulation during said encrypted WLAN communication;

wherein said first means is for performing the connection set-up by executing software-implemented instructions; and

wherein said second means comprises a single-purpose hardware device.